Aviso do APT40

Técnicas de espionagem do MSS da RPC em ação

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

Índice

Visão geral

Antecedentes

Este aviso, da autoria do Centro Australiano de Cibersegurança da Direção de Sinais da Austrália (ACSC da ASD), da Agência de Cibersegurança e Segurança das Infraestruturas dos Estados Unidos (CISA), da Agência de Segurança Nacional dos Estados Unidos (NSA), do Gabinete Federal de Investigação dos Estados Unidos (FBI), do Centro Nacional de Cibersegurança do Reino Unido (NCSC-UK), do Centro Canadiano de Cibersegurança (CCCS), do Centro Nacional de Cibersegurança da Nova Zelândia (NCSC-NZ), do Serviço Federal de Informações Alemão (BND) e do Gabinete Federal para a Proteção da Constituição (BfV), do Serviço Nacional de Informações da República da Coreia (NIS) e do Centro Nacional de Segurança Cibernética do NIS, e do Centro Nacional de Prontidão para Incidentes e Estratégia de Segurança Cibernética do Japão (NISC) e da Agência Nacional de Polícia (NPA) - a seguir designados por "agências autoras" - descrevem um grupo cibernético patrocinado pelo Estado da República Popular da China (RPC) e a sua atual ameaça às redes australianas. O aviso baseia-se no conhecimento comum das agências autoras sobre a ameaça, bem como nas investigações de resposta a incidentes da ACSC da ASD.

O grupo cibernético patrocinado pelo Estado da RPC já visou organizações em vários países, incluindo a Austrália e os Estados Unidos, e as técnicas abaixo indicadas são regularmente utilizadas por outros atores patrocinados pelo Estado da RPC a nível mundial. Portanto, as agências autoras acreditam que o grupo, e técnicas semelhantes, continuam a ser uma ameaça para as redes dos seus países.

As agências autoras consideram que este grupo efetua operações cibernéticas maliciosas para o Ministério da Segurança do Estado (MSS) da RPC. A atividade e as técnicas coincidem com os grupos identificados como Ameaça Persistente Avançada (Advanced Persistent Threat - APT) 40 (também conhecidos como Kryptonite Panda, GINGHAM TYPHOON, Leviathan e Bronze Mohawk nos relatórios da indústria). Este grupo foi anteriormente referido como estando sediado em Haikou, província de Hainan, RPC, e recebendo tarefas do MSS da RPC, Departamento de Segurança do Estado de Hainan.[2] O Aviso seguinte fornece uma amostra de estudos de caso significativos das técnicas deste adversário em ação contra duas redes vítimas. Os estudos de caso são importantes para os profissionais de cibersegurança a fim de poderem identificar, prevenir e remediar as intrusões do APT40 nas suas próprias redes. Os estudos de caso selecionados são aqueles em que foram tomadas medidas corretivas adequadas para reduzir o risco de reexploração por este agente de ameaça ou por outros. Como tal, os estudos de caso são naturalmente mais antigos, para garantir que as organizações tivessem o tempo necessário para remediar a situação.

Resumo de atividades

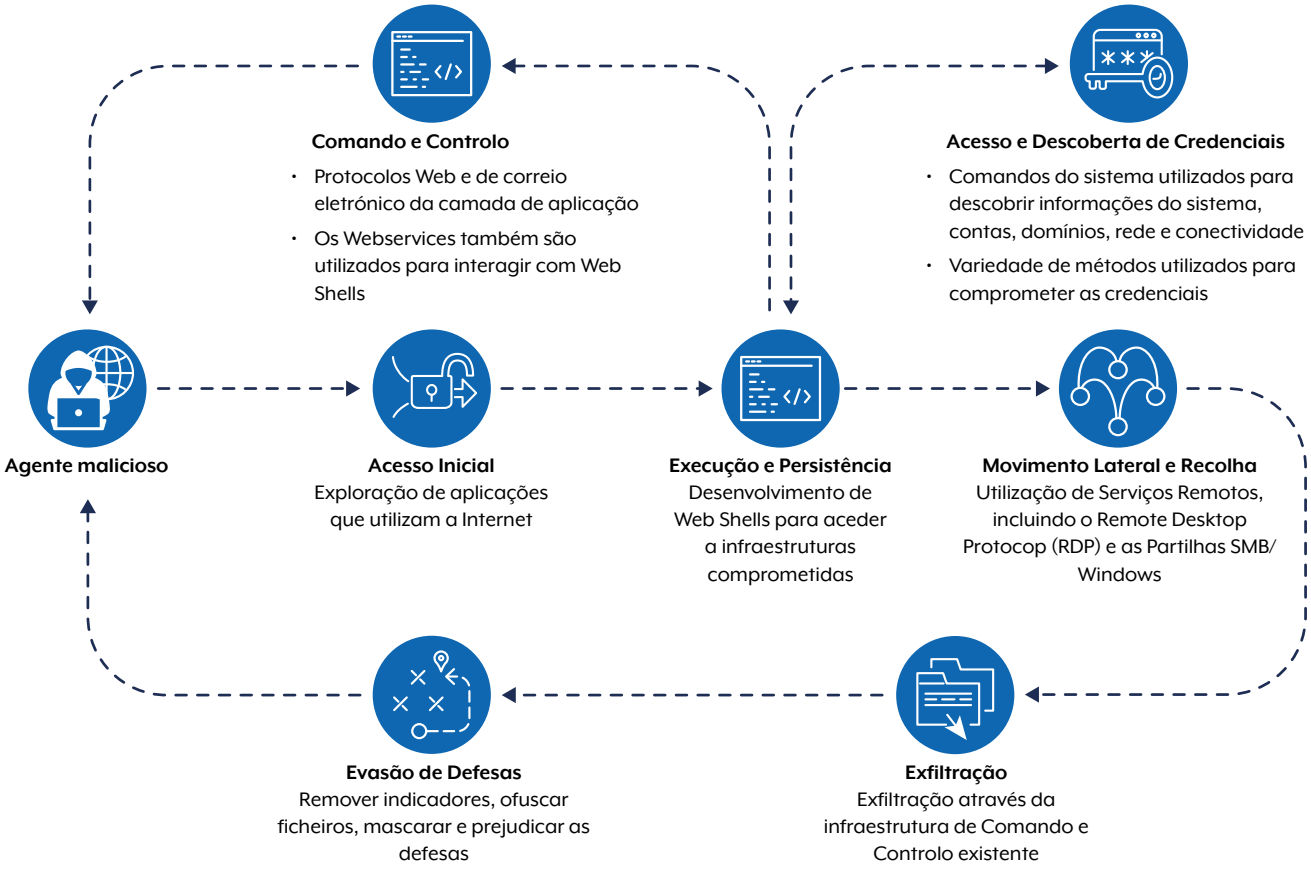
O APT40 tem visado repetidamente as redes australianas, bem como as redes do governo e do sector privado na região, e a ameaça que representam para as nossas redes é contínua. As técnicas descritas neste aviso são regularmente observadas contra redes australianas.

Nomeadamente, o APT40 possui a capacidade de transformar e adaptar rapidamente provas de conceito (POC) de exploração de novas vulnerabilidades e utilizá-las imediatamente contra redes-alvo que possuam a infraestrutura associada a essa vulnerabilidade. O APT40 realiza regularmente reconhecimentos contra redes de interesse, incluindo redes nos países das agências autoras, procurando oportunidades para comprometer os seus alvos. Este reconhecimento regular permite que o grupo identifique dispositivos vulneráveis, em fim de vida ou que já não são mantidos em redes de interesse, e que implante explorações rapidamente. O APT40 continua a ter sucesso na exploração de vulnerabilidades desde o início de 2017.

O APT40 explora rapidamente as novas vulnerabilidades públicas em software amplamente utilizado, como o Log4J Log4J (CVE 2021 44228), o Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) e Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473). O ACSC da ASD e as agências autoras esperam que o grupo continue a utilizar POCs para novas vulnerabilidades de alto perfil no prazo de horas ou dias após o lançamento público.

2 Departamento de Justiça dos EUA. 2021. Quatro cidadãos chineses que trabalhavam para o Ministério da Segurança do Estado acusados de uma Campanha Global de Intrusão Informática que visava a propriedade intelectual e informações comerciais confidenciais, incluindo a Investigação sobre Doenças Infecciosas.

Figura 1: Fluxograma TTP para a atividade do APT40



Parece que este grupo prefere a exploração de infraestruturas vulneráveis e públicas a técnicas que exijam a interação do utilizador, como as campanhas de phishing, e dá uma elevada prioridade à obtenção de credenciais válidas que permitam uma série de atividades subsequentes. O APT40 utiliza regularmente web shells (T1505.003) para persistência, particularmente no início do ciclo de vida de uma intrusão. Tipicamente, após o acesso inicial bem-sucedido, o APT40 foca em estabelecer a persistência a fim de manter o acesso no ambiente da vítima. No entanto, como a persistência ocorre no início de uma intrusão, é mais provável que seja observada em todas as intrusões - independentemente do grau de comprometimento ou de outras ações tomadas.

Técnicas de espionagem notáveis

Se bem que o APT40 tenha anteriormente utilizado sites australianos comprometidos como hosts de comando e controlo (C2) nas suas operações, o grupo desenvolveu esta técnica (T1594).

O APT40 adoptou a tendência global de utilizar dispositivos comprometidos, incluindo dispositivos SOHO (small-office/home-office), como infraestrutura operacional e redireccionadores de último acesso (T1584.008) para as suas operações na Austrália. Isto permitiu às agências autoras caracterizar e seguir melhor os movimentos deste grupo.

Muitos destes dispositivos SOHO estão em fim de vida ou não estão corrigidos e são um alvo fácil para a exploração N-day. Uma vez comprometidos, os dispositivos SOHO oferecem um ponto de lançamento para ataques concebidos para se misturarem com o tráfego legítimo e desafiarem os defensores da rede (T1001.003).

Esta técnica também é regularmente utilizada por outros atores patrocinados pelo Estado da RPC em todo o mundo, e as agências autoras consideram que se trata de uma ameaça partilhada. Para mais informações, consulte os avisos conjuntos People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices e PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.

O APT40 utiliza ocasionalmente infraestruturas adquiridas ou alugadas como infraestruturas C2 voltadas para as vítimas, nas suas operações; no entanto, esta técnica parece estar em declínio relativo.

Ferramentas

O ACSC da ASD está a partilhar alguns dos ficheiros maliciosos identificados durante as investigações descritas em seguida. Estes ficheiros foram carregados no VirusTotal para permitir que as comunidades de defesa de redes e de cibersegurança em geral entendam melhor as ameaças contra as quais se devem defender.

Estudos de casos

O ACSC da ASD está a partilhar dois relatórios de investigação anónimos para tornar conhecida a forma como os atores utilizam as suas ferramentas e técnicas.

MD5	Nome do ficheiro	Informação adicional
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java Source
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Java Bytecode
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Java Bytecode
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Java Source
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Java Bytecode
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Java Bytecode
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Java Bytecode
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Java Bytecode
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | Java Bytecode
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Java Source

Estudo de Caso 1

Este relatório foi tornado anónimo para permitir uma maior divulgação. A organização afetada é a seguir designada como "a organização". Alguns pormenores específicos foram retirados para proteger a identidade da vítima e os métodos de resposta a incidentes do ACSC da ASD.

Resumo executivo

Este relatório descreve as conclusões da investigação do ACSC da ASD sobre o comprometimento bem-sucedido da rede da organização entre julho e setembro de 2022. Este relatório de investigação foi fornecido à organização para resumir a atividade maliciosa observada e preparar recomendações de correção. Os resultados indicam que o compromisso foi realizado pelo APT40.

Em meados de agosto, o ACSC da ASD notificou a organização de interações maliciosas com a sua rede a partir de um dispositivo provavelmente comprometido que estava a ser utilizado pelo grupo em fins de agosto e, com o consentimento da organização, o ACSC da ASD instalou sensores baseados no host em hosts provavelmente afetados na rede da organização. Estes sensores permitiram que os analistas de resposta a incidentes do ACSC da ASD efetuassem uma investigação forense digital exaustiva. Utilizando os dados disponíveis dos sensores, os analistas do ACSC da ASD mapearam com sucesso a atividade do grupo e criaram uma cronologia detalhada dos eventos observados.

De julho a agosto, a atividade dos principais atores observada pelo ACSC da ASD incluiu:

- enumeração de hosts, que permite a um ator construir o seu próprio mapa da rede;
- utilização de web shell, dando ao ator uma posição inicial na rede e a capacidade de executar comandos; e
- implantação de outras ferramentas utilizadas pelo ator para fins maliciosos.

A investigação revelou provas de acesso a grandes quantidades de dados sensíveis e provas de que os atores se movimentavam lateralmente na rede (T1021.002). Grande parte do comprometimento foi facilitado pelo estabelecimento, pelo grupo, de múltiplos vectores de acesso à rede, pela estrutura plana da rede e pela utilização de software inseguro desenvolvido internamente que podia ser utilizado para carregar ficheiros arbitrariamente. Os dados exfiltrados incluíam credenciais de autenticação privilegiadas que permitiam ao grupo fazer login, bem como informações de rede que permitiriam aos atores recuperar o acesso não autorizado se o vetor de acesso original fosse bloqueado. Nenhumas ferramentas maliciosas adicionais foram descobertas para além das existentes na máquina inicialmente explorada; no entanto, o acesso de um grupo a credenciais legítimas e privilegiadas negaria a necessidade de ferramentas adicionais. Os resultados da investigação indicam que a organização foi provavelmente visada deliberadamente pelo APT40, em vez de ser vítima oportunista de uma vulnerabilidade conhecida publicamente.

Resultados da investigação

Em meados de agosto de 2022, o ACSC da ASD notificou a organização de que um IP malicioso confirmado, que se pensava que estava afiliado a um grupo cibernético patrocinado pelo Estado, tinha interagido com as redes informáticas da organização entre, pelo menos, julho e agosto. O dispositivo comprometido pertencia provavelmente a uma pequena empresa ou a um utilizador doméstico.

Em fins de agosto, o ACSC da ASD implantou um agente baseado em host em hosts da rede da organização que mostraram indícios de terem sido afetados pelo compromisso.

Alguns artefactos que poderiam ter apoiado os esforços de investigação não estavam disponíveis devido à configuração do registo ou à concepção da rede. Mesmo assim, a prontidão da organização em fornecer todos os dados disponíveis permitiu que os responsáveis pela resposta a incidentes do ACSC da ASD efetuassem uma análise exaustiva e compreendessem a provável atividade do APT40 na rede.

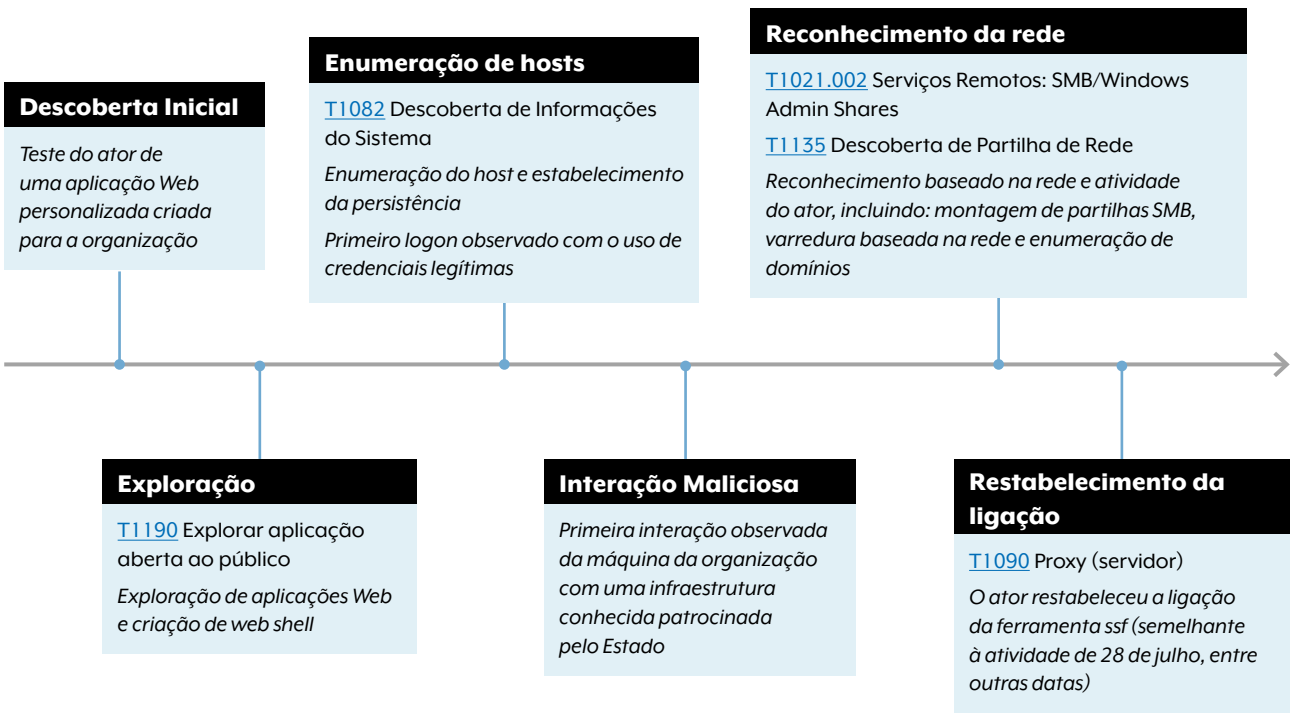
Em setembro, após consulta do ACSC da ASD, a organização decidiu retirar da lista os PI identificados na notificação inicial. Em outubro, a organização iniciou o processo de correção.

Detalhes

A partir de julho, os atores puderam testar e explorar uma aplicação web personalizada (T1190) executada em `<webapp>2-ext`, que permite ao grupo estabelecer uma base de apoio na zona desmilitarizada da rede (DMZ). Isto foi aproveitado para enumerar tanto a rede como todos os domínios visíveis. As credenciais comprometidas (T1078.002) foram usadas para consultar o Active Directory (T1018) e exfiltrar dados através da montagem de partilhas de ficheiros (T1039) a partir de várias máquinas dentro da DMZ. O ator efetuou um ataque Kerberoasting para obter credenciais de rede válidas de um servidor (T1558.003). Não se observou que o grupo tivesse ganho quaisquer pontos de presença adicionais, quer na DMZ, quer na rede interna.

Linha do tempo visual

A linha do tempo a seguir fornece uma visão geral das principais fases da atividade do ator malicioso observada na rede da organização.



Linha do tempo detalhada

Julho: Os atores estabeleceram uma ligação inicial à página inicial de uma aplicação web personalizada (T1190) criada para a organização (a seguir designada por "aplicação web" ou "*webapp*") através de uma ligação TLS (Transport Layer Security) (T1102). Não foi observada qualquer outra atividade digna de menção.

Julho: Os atores começam a enumerar o sítio web da aplicação web à procura de pontos finais[2] para investigar mais.

Julho: Os atores concentram-se nas tentativas de exploração de um ponto final específico.

Julho Os atores conseguem aceder com sucesso `POST` ao servidor Web, provavelmente através de um web shell colocado noutra página. Um segundo IP, provavelmente utilizado pelos mesmos atores, também começa a publicar no mesmo URL. Os atores criaram e testaram uma série de prováveis conchas da Web.

O método exato de exploração é desconhecido, mas é claro que o ponto final específico foi direcionado para criar ficheiros em `<webapp>2-ext`.

O ACSC da ASD acredita que as duas ligações de endereços IP faziam parte da mesma intrusão, devido ao seu interesse partilhado e ao facto de as ligações iniciais terem ocorrido com minutos de intervalo.

Julho: O grupo continua a efetuar a enumeração de hosts, procurando oportunidades de aumento de privilégios e implementando uma web shell diferente. Os atores iniciam sessão na aplicação web utilizando credenciais comprometidas para `<primeiro nome e apelido>@<domínio da organização>`.

Toda a atividade dos intervenientes não parece ter conseguido obter um aumento de privilégios em `<webapp>2-ext`. Em vez disso, os atores passaram a dedicar-se a atividades baseadas em redes.

Julho: O ator testa as credenciais comprometidas para uma conta de serviço[3] que provavelmente encontrou codificada em binários acessíveis internamente.

Julho: Os atores utilizam a ferramenta de código aberto Secure Socket Funnelling, que foi utilizada para se ligarem à infraestrutura maliciosa. Esta ligação é utilizada para canalizar o tráfego das máquinas de ataque do ator para as redes internas da organização, cujos nomes das máquinas são expostos nos registos de eventos quando tentam utilizar as credenciais da conta de serviço.

Agosto: Os atores são vistos a realizar uma quantidade limitada de atividades, incluindo não conseguir ligações envolvendo a conta de serviço.

Agosto: Os atores fazem uma enumeração significativa da rede e do Active Directory. Uma conta comprometida diferente é subsequentemente utilizada para montar partilhas[4] em máquinas Windows dentro da DMZ, permitindo a exfiltração de dados com sucesso.

Este parece ser um uso oportunista de uma credencial roubada em máquinas montáveis na DMZ. As firewalls impediram o ator de visar a rede interna com atividade semelhante.

Agosto - Setembro: A ferramenta SSF restabeleceu uma ligação a um IP malicioso. Não se observou o grupo a realizar quaisquer atividades adicionais até o seu acesso ser bloqueado.

Setembro: A organização bloqueia o IP malicioso, colocando-o na lista negra das suas firewalls.

2 Neste contexto, um endpoint é uma função da aplicação web

3 As contas de serviço não estão ligadas a utilizadores individuais, mas sim a serviços. Num domínio empresarial Microsoft, existem vários tipos de contas.

4 A montagem de partilhas é o processo de tornar os ficheiros numa estrutura de sistema de ficheiros acessíveis a um utilizador ou grupo de utilizadores.

Táticas e técnicas dos atores

A estrutura MITRE ATT&CK é uma coleção documentada de táticas e técnicas utilizadas por agentes de ameaças no ciberespaço. O quadro foi criado pela empresa norte-americana sem fins lucrativos The MITRE Corporation e funciona como uma linguagem global comum sobre o comportamento dos agentes de ameaça.

O ACSC da ASD avalia as seguintes técnicas e táticas como sendo relevantes para a atividade maliciosa do ator:

Reconhecimento

T1594 – Pesquisar sítios web pertencentes às vítimas

O ator enumerou o sítio web da aplicação web personalizada para identificar oportunidades de acesso à rede.

Acesso Inicial

T1190 – Explorar a aplicação voltada para o público (relativamente à exploração da aplicação Web personalizada)

T1078.002 – Contas válidas: Contas de domínio (relativamente ao início de sessão com credenciais incluídas)

A exploração de aplicações web personalizadas expostas à Internet constituiu um ponto de acesso inicial para o ator. O ator conseguiu posteriormente utilizar as credenciais que tinha comprometido para continuar a aceder à rede.

Execução

T1059 – Interpretador de comandos e scripts (relativo à execução de comandos através do web shell)

T1072 – Ferramentas de implantação de software (relativamente ao ator que utiliza a ferramenta de código aberto Secure Socket Funnelling (SSF) para se ligar a um IP)

Persistência

T1505.003 – Componente de Software do Servidor: Web Shell (relativo ao uso de um web shell e SSF para estabelecer acesso)

Acesso a credenciais

T1552.001 – Credenciais dos armazenamentos de senhas (relativas a ficheiros de senhas relacionados com o sistema de gestão de edifícios (BMS))

T1558.003 – Roubar ou falsificar bilhetes Kerberos: Kerberoasting (relativo a um ataque para obter credenciais de rede)

Movimento lateral

T1021.002 – Serviços Remotos: Partilhas SMB (relativamente ao ator que monta partilhas SMB a partir de vários dispositivos)

Recolha

T1213 – Dados dos repositórios de informação (relativos a manuais/documentação encontrados no servidor BMS)

Exfiltração

T1041 – Exfiltração através do canal C2 (relativamente à exfiltração de dados pelo ator a partir do Active Directory e das partilhas montadas)

Estudo de caso 2

Este relatório foi anonimizadoo para permitir uma maior divulgação. A organização afetada é a seguir designada por 'a organização'. Alguns pormenores específicos foram retirados para proteger a identidade da vítima e os métodos de resposta a incidentes do ACSC da ASD.

Resumo executivo

Este relatório detalha as conclusões da investigação do ACSC da ASD sobre o comprometimento bem-sucedido da rede da organização em abril de 2022. Este relatório de investigação foi fornecido à organização para resumir a atividade maliciosa observada e enquadrar as recomendações de correção. As conclusões indicam que o compromisso foi efetuado pela APT40.

Em maio de 2022, o ACSC da ASD notificou uma organização sobre uma suspeita de atividade maliciosa que afetava a rede da organização desde abril de 2022. Subsequentemente, a organização informou o ACSC da ASD de que tinha descoberto software malicioso num servidor voltado para a Internet que fornecia o portal de início de sessão para a solução de acesso remoto empresarial da organização. Este servidor utilizava um produto de login de acesso remoto e gestão de identidade e será referido neste relatório como 'o aparelho comprometido'. Este relatório apresenta em detalhe as conclusões da investigação e os conselhos de correção elaborados para a organização em resposta à investigação realizada pelo ACSC da ASD.

As provas indicavam que parte da rede da organização tinha sido comprometida por cibercriminosos através do portal de início de sessão de acesso remoto da organização desde, pelo menos, abril de 2022. Este servidor pode ter sido comprometido por vários atores e foi provavelmente afetado por uma vulnerabilidade de execução remota de código (RCE) que foi amplamente divulgada na altura do compromisso.

As principais atividades dos atores observadas pelo ACSC da ASD incluíram:

- enumeração de hosts, que permite a um ator construir o seu próprio mapa da rede;
- exploração de aplicações orientadas para a Internet e utilização do web shell, dando ao ator uma posição inicial na rede e a capacidade de executar comandos;
- exploração de vulnerabilidades de software para elevar os privilégios; e
- recolha de credenciais para permitir movimentos laterais

O ACSC da ASD descobriu que um agente malicioso tinha exfiltrado várias centenas de pares de nomes de utilizador e palavras-passe únicos no aparelho comprometido em abril de 2022, como também uma série de códigos de autenticação multifactor e artefactos técnicos relacionados com sessões de acesso remoto. Após uma análise pela organização, verificou-se que as palavras-passe eram legítimas. O ACSC da ASD avalia que o ator pode ter recolhido estes artefactos técnicos para sequestrar ou criar uma sessão de início de sessão remota como um utilizador legítimo e aceder à rede empresarial interna da organização utilizando uma conta de utilizador legítima.

Resultados da investigação

Resumo da investigação

O ACSC da ASD determinou que o ator comprometeu o(s) aparelho(s) que fornece(m) sessões de início de sessão à distância ao pessoal da organização e utilizou este compromisso para tentar realizar novas atividades. Estes aparelhos são compostos por três hosts de balanceamento de carga onde foram detetados os primeiros indícios de comprometimento. A organização desligou dois dos três hosts de carga equilibrada pouco depois do comprometimento inicial. Como resultado, toda a atividade subsequente ocorreu num único host. Os outros servidores associados ao aparelho comprometido também foram balanceados de forma semelhante. Para efeitos de legibilidade, todos os aparelhos comprometidos são referidos na maior parte deste relatório como um "aparelho único".

Acredita-se que o ator tenha usado vulnerabilidades conhecidas publicamente para implantar web shells no dispositivo comprometido a partir de abril de 2022. Considera-se que os agentes de ameaças do grupo obtiveram privilégios acrescidos no aparelho. O ACSC da ASD não conseguiu determinar a extensão total da atividade devido à falta de disponibilidade de registos. No entanto, as evidências no dispositivo indicam que um ator conseguiu o seguinte:

- A recolha de várias centenas de pares de nomes de utilizador e palavras-passe genuínas; e
- A coleção de artefactos técnicos que podem ter permitido a um agente malicioso aceder a uma sessão de infraestrutura de ambiente de trabalho virtual (VDI) como um utilizador legítimo.

O ACSC da ASD avalia que o ator teria procurado comprometer ainda mais a rede da organização. Os artefactos exfiltrados pelo ator podem ter-lhe permitido desviar ou iniciar sessões de ambiente de trabalho virtual como um utilizador legítimo, possivelmente como um utilizador de sua escolha, incluindo administradores. O ator pode ter utilizado este vetor de acesso para comprometer ainda mais os serviços da organização, a fim de alcançar a persistência e outros objetivos.

Outros aparelhos da organização no ambiente gerido pelo fornecedor de serviços de alojamento virtual não apresentavam indícios de comprometimento.

Acesso

O host com a aplicação comprometida fornecia autenticação através do Active Directory e de um servidor Web, para os utilizadores que se ligavam a sessões VDI (T1021.001).

Localização	Nomes de host de aparelhos comprometidos (com equilíbrio de carga)
Datacentre 1	HOST1, HOST2, HOST3

A infraestrutura do dispositivo também incluía hosts de gateway de acesso que fornecem um túnel para a VDI para o utilizador, uma vez que este possui um token de autenticação gerado e descarregado do dispositivo.

Não havia evidências de comprometimento de nenhum desses hosts. No entanto, os registos dos hosts do gateway de acesso mostraram indícios de interações significativas com endereços IP maliciosos conhecidos. Provavelmente isso reflecte a atividade que ocorreu neste host, ou as ligações de rede com a infraestrutura do ator de ameaça que chegou a este host. A natureza desta atividade não pôde ser determinada com base nas provas disponíveis, mas indica que o grupo procurou deslocar-se lateralmente na rede da organização (TA0008).

Hosts internos

O ACSC da ASD investigou dados limitados do segmento de rede da organização interna. As atividades maliciosas, tentadas ou bem-sucedidas, que se sabe terem afetado o segmento de rede da organização interna incluem o acesso de um ator a artefactos relacionados com VDI, a exploração de um servidor SQL interno (T1505.001) e o tráfego inexplicável observado a partir de endereços IP maliciosos conhecidos através dos dispositivos de gateway de acesso (TA0011).

Utilizando o seu acesso ao dispositivo comprometido, o grupo recolheu nomes de utilizador genuínos, palavras-passe (T1003) e valores de token MFA (T1111). O grupo também recolheu JSON Web Tokens (JWTs) (T1528), que é um artefacto de autenticação utilizado para criar sessões de início de sessão em ambientes de trabalho virtuais. O ator poderá ter conseguido utilizá-lo para criar ou desviar sessões de ambiente de trabalho virtual (T1563.002) e aceder ao

segmento de rede interno da organização como um utilizador legítimo (T1078).

O ator também utilizou o acesso à aplicação comprometida para aceder a um servidor SQL (T1505.001), que residia na rede interna da organização. É provável que o ator tenha tido acesso a esses dados.

As provas disponíveis a partir do dispositivo de gateway de acesso revelaram que o tráfego de rede ocorreu através de ou para este dispositivo a partir de endereços IP maliciosos conhecidos. Tal como descrito acima, isto pode indicar que os ciber-atores maliciosos tiveram impacto ou utilizaram este dispositivo, potencialmente para penetrar na rede interna.

Linha do tempo da investigação

A lista seguinte apresenta um calendário com as principais atividades descobertas durante a investigação.

Tempo	Evento
Abril de 2022	Endereços IP maliciosos conhecidos interagem com o host do gateway de acesso HOST7. Não foi possível determinar a natureza das interações.
Abril de 2022	Todos os hosts, HOST1, HOST2 e HOST3, foram comprometidos por um ou mais atores maliciosos, e foram colocados web shells nos hosts. Foi criado ou modificado um ficheiro de registo no HOST2. Este ficheiro contém material de credenciais provavelmente capturado por um ator malicioso. Os ficheiros /etc/security/opasswd e /etc/shadow foram modificados no HOST1 e no HOST3, indicando que as palavras-passe foram alteradas. As ecidências disponíveis no HOST1 sugerem que a palavra-passe do utilizador 'sshuser' foi alterada.
Abril de 2022	O HOST2 foi desligado pela organização. Foram criados web shells adicionais (T1505.003) em HOST1 e HOST3. O HOST1 sofreu tentativas de força bruta SSH por parte do HOST3. Um ficheiro de registo foi modificado (T1070) no HOST3. Este ficheiro contém material de credenciais (T1078) provavelmente capturado por um ator malicioso. Os JWTs foram capturados (T1528) e enviados para um ficheiro no HOST3. O HOST3 foi desligado pela organização. A partir deste momento, toda a atividade ocorre noHOST1.
Abril de 2022	Foram criados web shells adicionais no HOST1 (T1505.003). Os JWTs foram capturados e enviados para um ficheiro no HOST1.
Abril de 2022	São criadas web shells adicionais no HOST1 (T1505.003), e um endereço IP malicioso conhecido interage com o host (TA0011). Um endereço IP malicioso conhecido interage com o host do gateway de acesso HOST7.
Maio de 2022	Um endereço IP malicioso conhecido interagiu com o host do gateway de acesso HOST7 (TA0011). Um evento de autenticação para um utilizador está ligado a um endereço IP malicioso conhecido nos registos do HOST1. Um web shell adicional é criado neste host (T1505.003).
Maio de 2022	Um script em HOST1 foi modificado por um ator (T1543). Este script contém uma funcionalidade que teria extraído dados de um servidor SQL interno.
Maio de 2022	Um ficheiro de registo adicional no HOST1 foi modificado pela última vez (T1070). Este ficheiro contém pares de nome de utilizador e palavra-passe para a rede da organização, que se acredita serem legítimos (T1078).
Maio de 2022	Um ficheiro de registo adicional foi modificado pela última vez (T1070). Este ficheiro contém JWTs recolhidos de HOST1.
Maio de 2022	Foram criados outros web shells no HOST1 (T1505.003). Nesta data, a organização relatou a descoberta de um web shell com data de criação em abril de 2022 para o ACSC da ASD
Maio de 2022	Vários scripts foram criados no HOST1, incluindo um chamado Log4jHotPatch.jar.
Maio de 2022	O comando iptables-save foi usado para adicionar duas portas abertas ao host do gateway de acesso. As portas eram 9998 e 9999 (T1572).

Táticas e técnicas do ator

Destacam-se a seguir várias táticas e técnicas identificadas durante a investigação.

Acesso Inicial

T1190 Explorar aplicação voltada para o público

O grupo explorou provavelmente vulnerabilidades de RCE, escalonamento de privilégios e desvio de autenticação no produto de login de acesso remoto e gestão de identidades para obter acesso inicial à rede.

Este método de acesso inicial é considerado o mais provável devido ao seguinte:

- O servidor estava vulnerável a esses CVE na altura;
- Tentativas de explorar essas vulnerabilidades a partir de infraestruturas de atores conhecidos; e
- A primeira atividade maliciosa interna conhecida ocorreu pouco depois das tentativas de exploração.

Execução

T1059.004 Interpretador de comandos e scripts: Unix Shell

O grupo que explorou com sucesso as vulnerabilidades acima pode ter sido capaz de executar comandos num Unix shell disponível no aparelho afetado. Não é possível fornecer detalhes completos sobre os comandos executados pelos atores, uma vez que não foram registados pelo aparelho.

Persistência

T1505.003 Componente de Software do Servidor: Web Shell

Os atores implantaram vários web shells no aparelho afetado. É possível que vários atores distintos tenham implantado web shells, mas que apenas um pequeno número de atores tenha efetuado atividades utilizando esses web shells. Os web shells teriam permitido a execução arbitrária de comandos pelo ator nos aparelhos comprometidos.

Escalada de privilégios

T1068 Exploração para Escalada de Privilégios

As provas disponíveis não descrevem o nível de privilégio atingido pelos atores. No entanto, usando web shells, os atores teriam alcançado um nível de privilégio comparável ao do servidor web no aparelho comprometido. As vulnerabilidades que se acredita estarem presentes no aparelho comprometido teriam permitido aos atores obter privilégios de root.

Acesso às credenciais

T1056.003 Captura de entrada: Captura do portal Web

As evidências no aparelho comprometido mostraram que o ator tinha capturado várias centenas de pares de palavras-passe de nome de utilizador, em texto claro, que se acredita serem legítimos. Provavelmente esses foram capturados através de alguma modificação do processo de autenticação genuíno que envia as credenciais para um ficheiro.

T1111 Interceção de autenticação multi-fator

O ator também capturou o valor dos tokens MFA correspondentes a logins legítimos. Estes foram provavelmente capturados através da modificação do processo de autenticação genuíno para enviar estes valores para um ficheiro. Não há evidências de comprometimento do 'servidor secreto' que armazena os valores únicos que garantem a segurança dos tokens MFA.

T1040 Monitorização de Rede

Acredita-se que o ator tenha capturado JWTs capturando o tráfego HTTP no dispositivo comprometido. Há evidências de que o utilitário tcpdump foi executado no aparelho comprometido, o que pode ter sido a forma como o ator capturou estes JWTs.

T1539 Roubar Cookie de Sessão Web

Como descrito acima, o ator capturou JWTs, que são análogos aos cookies de sessão web. Estes poderiam ter sido reutilizados pelo ator para estabelecer mais acessos.

Descoberta

T1046 Descoberta de Serviços de Rede

Há evidências de que o utilitário de pesquisa de rede nmap foi executado no aparelho comprometido para pesquisar outros aparelhos no mesmo segmento de rede. Este foi provavelmente utilizado pelo ator para descobrir outros serviços de rede acessíveis que poderiam apresentar oportunidades de movimento lateral.

Recolha

As evidências disponíveis não revelam como os intervenientes recolheram os dados ou o que foi exatamente recolhido do dispositivo comprometido ou de outros sistemas. No entanto, é provável que os intervenientes tenham tido acesso a todos os ficheiros do dispositivo comprometido, incluindo as credenciais capturadas (T1003), os valores do token MFA (T1111) e os JWTs descritos acima.

Comando e Controlo

T1071.001 Protocolo da camada de aplicação: Protocolos da Web

Os atores utilizavam os web shells para comando e controlo. Os comandos dos web shells teriam sido transmitidos através de HTTPS utilizando o servidor Web existente no aparelho (T1572).

T1001.003 Ofuscação de dados: Representação de protocolo

Os atores utilizaram dispositivos comprometidos como ponto de lançamento para ataques concebidos para se misturarem com o tráfego legítimo.

Recomendações de deteção e atenuação

O ACSC da ASD recomenda vivamente a implementação dos Oito Essenciais Controlos e Estratégias para mitigar incidentes de cibersegurança associados. Seguem-se recomendações para acções de segurança de rede que devem ser tomadas para detetar e prevenir intrusões pela APT40, seguidas de mitigações específicas para quatro TTPs chave resumidas na Tabela 1.

Deteção

Alguns dos ficheiros identificados acima foram colocados em locais como C:\Users\Public* e C:\Windows\Temp*. Estas localizações podem ser pontos convenientes para escrever dados, uma vez que são normalmente graváveis por todos, ou seja, todas as contas de utilizador registadas no Windows têm acesso a estes diretórios e aos seus subdirectórios. Muitas vezes, qualquer utilizador pode posteriormente aceder a estes ficheiros, permitindo oportunidades de movimento lateral, evasão à defesa, execução com poucos privilégios e preparação para a exfiltração.

As seguintes regras Sigma procuram a execução a partir de localizações suspeitas como um indicador de atividade anómala. Em todos os casos, é necessária uma investigação subsequente para confirmar a atividade maliciosa e a atribuição.

Título: Execução Mundial Gravável - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Descrição: Detetar a execução do processo a partir de C:\Windows\Temp.

Antecedentes:

Esta regra procura especificamente a execução a partir de C:\Windows\Temp*. Temp é mais amplamente utilizado por aplicações benignas e, por isso, um indicador malicioso de menor confiança do que a execução a partir de outros subdirectórios graváveis a nível mundial em C:\Windows.

A remoção de aplicações executadas pelos utilizadores SYSTEM ou NETWORK SERVICE reduz substancialmente a quantidade de atividade benigna selecionada por esta regra.

Isto significa que a regra pode não detetar execuções maliciosas com um nível de privilégio mais elevado, mas recomenda-se a utilização de outras regras para determinar se um utilizador está a tentar elevar os privilégios para SISTEMA.

Investigação:

1. Examinar as informações diretamente associadas à execução deste ficheiro, tais como o contexto do utilizador, o nível de integridade da execução, a atividade de seguimento imediata e as imagens carregadas pelo ficheiro.
2. Investigar o processo contextual, a rede, o ficheiro e outros dados de suporte no host para ajudar a avaliar se a atividade é maliciosa.
3. Se necessário, tentar recolher uma cópia do ficheiro para engenharia inversa, a fim de determinar se é legítimo.

Referências:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Autor: ACSC do ASD

Data: 2024/06/19

Status: experimental

Tags:

- tlp.green
- classification.au.official
- attack.execution

Fonte de registo:

```
categoria: processo_criação
produto: Windows
```

Deteção

```
temp:
    Imagem|startswith: 'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase: 'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
system_user:
    Utilizador:
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

condition: temp and not (common_temp_path or system_user or dismhost or known_parent)

Falsos positivos:

- As aplicações de auditoria da lista de permissões foram observadas a efetuar executáveis de Temp.
- O Temp conterá legitimamente um conjunto de aplicações de configuração e lançadores, por isso valerá a pena considerar a prevalência deste comportamento numa rede monitorizada (e se pode ou não ser incluído na lista de permissões) antes de implementar esta regra.

Nível: low

Título: Execução Mundial Gravável - Non-Temp Subdiretório do sistema

ID 5b187157-e892-4fc9-84fc-aa48aff9f997

Descrição: Detetar a execução de processos a partir de uma localização gravável por todos num subdiretório da localização de instalação do SO Windows.

Antecedentes:

Esta regra procura especificamente a execução a partir de diretórios graváveis a nível mundial dentro de C:\ e particularmente C:\Windows*, com a exceção de C:\Windows\Temp (que é mais amplamente utilizado por aplicações benignas e, portanto, um indicador malicioso de menor confiança).

As pastas AppData são excluídas se um ficheiro for executado como SYSTEM - esta é uma forma benigna pela qual muitos ficheiros temporários de aplicações são executados.

Depois de completar uma linha de base de rede inicial e identificar execuções benignas conhecidas a partir destas localizações, esta regra raramente deve ser ativada.

Investigação:

1. Examinar as informações diretamente associadas à execução deste ficheiro, tais como o contexto do utilizador, o nível de integridade da execução, a atividade de seguimento imediata e as imagens carregadas pelo ficheiro.
2. Investigar o processo contextual, a rede, o ficheiro e outros dados de suporte no host para ajudar a avaliar se a atividade é maliciosa.
3. Se necessário, tentar recolher uma cópia do ficheiro para engenharia inversa, a fim de determinar se é legítimo.

Referências:

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Autor: ACSC do ASD

Data: 2024/06/19
Status: experimental

Tags:

- tlp.green
- classification.au.official
- attack.execution

Fonte de registo:

categoria: processo_criação
produto: windows

Deteção

writable_path:

Image|contains:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'

- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'
- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Image|contains: '\\AppData\\'
Utilizador: 'SYSTEM'

condição: writable_path and not appdata

Falsos positivos:

As aplicações de auditoria da lista de permissões foram observadas a efetuar executáveis de Temp.

É palusível que os scripts e ferramentas administrativas usadas no ambiente monitorizado possam ser localizados num desses diretórios e devem ser resolvidos caso a caso.

Nível: alto

Título: Execução Mundial Gravável - Ustilizadores

ID: 6dda3843-182a-4214-9263-925a80b4c634

Descrição: Detetar a execução do processo de C:\Users\Public* e outras pastas graváveis por todos entre os Utilizadores.

Antecedentes:

As pastas AppData estão excluídas se um ficheiro for executado como SYSTEM – está é uma maneira benigna em que muitos ficheiros temporários de aplicação são executados.

Investigação:

1. Analisar a informação diretamente associada com a execução deste ficheiro, tal como o contexto do utilizador, nível de integridade da execução, atividade de seguimento imediato e imagens carregadas pelo ficheiro.
2. Investigar o processo contextual, a rede, o ficheiro e outros dados de suporte no host para ajudar a avaliar se a atividade é maliciosa.
3. Se necessário, tentar recolher uma cópia do ficheiro para engenharia inversa, a fim de determinar se é legítimo.

Referências

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Autor: ACSC do ASD

Data: 2024-06-19

Status: experimental

Tags:

- tlp.green
- classification.au.official
- attack.execution

Fonte de registo:

categoria: processo_criação

produto: Windows

Deteção:

Utilizadores:

Image|contains:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:

Image|contains: '\\AppData\\'

Utilizador: 'SYSTEM'

condição: utilizadores e não appdata

Falsos positivos:

- É palusível que os scripts e ferramentas administrativas usadas no ambiente monitorizado possam ser localizados em Public ou num subdiretório e devem ser resolvidos caso a caso.

Nível: médio

Mitigações

Logging

Durante as investigações do ACSC do ASD, uma questão comum que reduz a eficácia e rapidez dos esforços de investigação é a falta de informação de registo exaustivo e histórico ao longo de várias áreas incluindo registos de solicitação do servidor web, registos de eventos Windows e registos de proxy da internet.

O ACSC do ASD recomenda rever e implementar suas orientações sobre Registo e Reenvio de Eventos do Windows incluindo os ficheiros de configuração e scripts no Repositório de Logs de Eventos do Windows e as Orientações para Monitorização de Sistemas do Manual de Segurança da Informação, para incluir a centralização e retenção de registos por um período apropriado.

Gestão de patches

Corrija rapidamente todos os dispositivos e serviços expostos à internet, incluindo servidores web, aplicações web e gateways de acesso remoto. Considere implementar um sistema de gestão de patches centralizado para automatizar e apressar o processo. O ACSC do ASD recomenda a implementação das Orientações para Monitorização de Sistemas do ISM, especificamente, os controlos de Patching de Sistemas quando aplicável.

A maioria dos exploits utilizados pelo ator eram conhecidos publicamente e tinham correções ou mitigações disponíveis. As organizações devem assegurar que patches de segurança ou mitigação são aplicados à infraestrutura voltada para a internet dentro de 48 horas, e quando possível, utilizar as versões de software e sistemas operacionais mais atualizados.

Segmentação da rede

A segmentação da rede pode dificultar significativamente a localização e o acesso dos adversários aos dados confidenciais das organizações. Segmente a rede para limitar ou bloquear movimento lateral negando o tráfego entre computadores salvo necessário. Servidores importantes como Active Directory e outros servidores de autenticação devem ser passíveis de serem administrados somente por um número limitado de servidores intermediários ou "servidores de salto". Estes servidores devem ser monitorizados de perto, bem protegidos e limitarem os utilizadores e dispositivos que podem conectar com eles.

Independentemente dos casos identificados em que o movimento lateral é impedido, a segmentação adicional da rede poderá limitar ainda mais a quantidade de dados a que os atores poderão aceder e extrair.

Mitigações adicionais

As agências autoras também recomendam as mitigações seguintes para combater o uso por APT40 e outros dos TTPs a seguir.

- Desative serviços de rede, portas e protocolos não utilizados ou desnecessários.
- Utilize firewalls de aplicações web (WAFs) bem ajustados para proteger os servidores e aplicações web.
- Aplique o princípio do menor privilégio para limitar o acesso a servidores, partilhas de ficheiros, e outros recursos.
- Utilize a autenticação multifator (MFA) e contas de serviço geridas para que as credenciais sejam mais difíceis de decifrar e reusar. A MFA deve ser aplicada a todos os serviços de acesso remoto acessíveis pela internet, incluindo:
  - E-mail baseado na web e em nuvem
  - Plataformas de colaboração
  - Conexões de rede privada virtual
  - Serviços de Área de Trabalho Remota
- Substituir equipamentos em fim de vida útil.

Tabela 1. Estratégias/Técnicas de Mitigação

TTP	Oito Estratégias Essenciais de Mitigação	Controlos ISM
Acesso Inicial T1190 Exploração de aplicação voltada ao público	Aplicações de patches Sistemas operacionais de patches Autenticação multifactor Controlo de aplicações	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Execução T1059 Interpretador de comandos e scripts	Controlo de aplicações Restringir macros do Microsoft Office Restringir privilégios administrativos	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Persistência T1505.003 Componente de Software do Servidor: Web Shell	Controlo de aplicações Restringir privilégios administrativos	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Acesso Inicial / Escalada de Privilégios / Persistência T1078 Contas válidas	Sistemas operacionais de patches Autenticação multifactor Restringir privilégios administrativos Controlo de aplicações Endurecimento de aplicações de usuário	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

Para aconselhamento adicional sobre deteção e mitigação em geral, consulte as secções Mitigações e Deteções na página web de técnica MITRE ATT&CK para cada uma das técnicas identificadasno resumo MITRE ATT&CK no final deste aviso.

Isenção de responsabilidade

A informação contida nesta orientação está a ser fornecida 'tal como é', apenas para fins informativos. As agências autoras não endossam nenhuma entidade, produto, empresa ou serviço comerciais, incluindo quaisquer entidades, produtos ou serviços vinculados neste documento. Qualquer referência a entidades comerciais, produtos, processos ou serviços específicos por marca de serviço, marca registada, fabricante ou de outra forma, não constitui nem implica endosso, recomendação ou preferência por parte das agências autoras.

Este documento está marcado como TLP:LIVRE. A divulgação não é limitada. As fontes podem usar TLP:LIVRE quando a informação acarreta risco mínimo ou nenhum risco previsível de uso indevido, de acordo com as regras e os procedimentos aplicáveis à divulgação pública. Sujeito às regras padrão de direitos autorais, a informação TLP:LIVRE pode ser distribuída sem restrição. Para mais informações sobre o Protocolo de Semáforo (Traffic Light Protocol), ver cisa.gov/tlp

MITRE ATT&CK – Espionagem de interesse histórico APT40

Reconhecimento (TA0043)	
Pesquisar Sites de Propriedade de Vítimas (T1594)	Recolher Informações sobre a Identitidade de Vítimas: Credenciais (T1589.001)
Digitalização Ativa: Digitalização da Vulnerabilidade (T1595.002)	Recolher Informações sobre o Host de Vítimas (T1592)
Pesquisar Sites/Domínios Abertos: Motores de Busca (T1593.002)	Recolher Informações sobre a Rede de Vítimas: Propriedades de Domínio (T1590.001)
Recolher Informações sobre a Identitidade de Vítimas: Endereços Eletrónicos (T1589.002)	

Desenvolvimento de Recursos (TA0042)	
Adquirir Infraestrutura: Domínios (T1583.001)	Adquirir Infraestrutura (T1583)
Adquirir Infraestrutura: Servidor DNS (T1583.002)	Comprometer Contas (T1586)
Desenvolver capacidades: Certificados de Assinatura de Código (T1587.002)	Comprometer Infraestrutura (T1584)
Desenvolver capacidades: Certificados Digitais (T1587.003)	Desenvolver capacidades: Malware (T1587.001)
Obter Capacidades: Certificados de Assinatura de Código (T1588.003)	Criar Contas: Contas na Nuvem (T1585.003)
Comprometer Infraestrutura: Dispositivos de Rede (T1584.008)	Obter Capacidades: Certificados Digitais (T1588.004)

Acesso Inicial (TA0001)	
Contas Válidas (T1078)	Phishing (T1566)
Contas Válidas: Contas predefinidas(T1078.001)	Phishing: Anexo de Spearphishing (T1566.001)
Contas Válidas: Contas de Domínio (T1078.002)	Phishing: Link de Spearphishing (T1566.002)
Serviços Remotos Externos (T1133)	Explorar aplicação aberta ao público (T1190)
Comprometimento por drive-by (T1189)	

Execução (TA0002)	
Instrumentação de Gestão do Windows (T1047)	Interpretador de comandos e scripts: Python (T1059.006)
Trabalho/Tarefa Programados: At (T1053.002)	Interpretador de comandos e scripts: JavaScript (T1059.007)
Trabalho/Tarefa Programados: Tarefa Programada (T1053.005)	API Nativa (T1106)
Interpretador de comandos e scripts (T1059)	Comunicação Inter-Processos (T1559)
Interpretador de comandos e scripts: Shell de Comando do Windows (T1059.003)	Serviços do Sistema: Execução de Serviço (T1569.002)
Interpretador de comandos e scripts: PowerShell (T1059.001)	Exploração para Execução do Cliente (T1203)
Interpretador de comandos e scripts: Visual Basic (T1059.005)	Execução do utilizador: Ficheiro Malicioso (T1204.002)
Interpretador de comandos e scripts: Unix Shell (T1059.004)	Interpretador de comandos e scripts: Apple Script (T1059.002)
Trabalho/Tarefa Programados: Cron (T1053.003)	Ferramentas de Implementação de Software (T1072)

Persistência (TA0003)	
Contas Válidas (T1078)	Componente de Software do Servidor: Web Shell (T1505.003)
Inicialização da Aplicação Office: Macros de Modelos do Office (T1137.001)	Criar ou Modificar Processo de Sistema: Serviço do Windows (T1543.003)
Trabalho/Tarefa Programados: At (T1053.002)	Execução de Inicialização automática de inicialização ou logon: Chaves de Execução do Registo / Pasta de Inicialização (T1547.001)
Trabalho/Tarefa Programados: Tarefa Programada (T1053.005)	Execução de Inicialização automática de inicialização ou logon: Modificação de Atalho (T1547.009)
Serviços Remotos Externos (T1133)	Fluxo de Execução de Sequestro: Sequestro de ordem de pesquisa de DLL (T1574.001)
Trabalho/Tarefa Programada: Cron (T1053.003)	Fluxo de Execução de Sequestro: Carregamento lateral do DLL (T1574.002)
Manipulação de Contas (T1098)	Contas Válidas: Contas em Nuvem (T1078.004)
Contas Válidas: Contas de Domínio (T1078.002)	

Escalada de Privilégio (TA0004)	
Trabalho/Tarefa Programada: At (T1053.002)	Criar ou Modificar Processo de Sistema: Serviço do Windows (T1543.003)
Trabalho/Tarefa Programada: Tarefa Programada (T1053.005)	Execução de Inicialização automática de inicialização ou logon: Chaves de Execução do Registo / Pasta de Inicialização (T1547.001)
Injeção de Processo: Sequestro de Execução de Thread (T1055.003)	Execução de Inicialização automática de inicialização ou logon: Modificação de Atalho (T1547.009)
Injeção de Processo: Escavação de Processo (T1055.012)	Fluxo de Execução de Sequestro: Sequestro de ordem de pesquisa de DLL (T1574.001)

Escalada de Privilégio (TA0004)	
Contas Válidas: Contas de Domínio (T1078.002)	Exploração para Escalada de Privilégios (T1068)
Manipulação de Token de Acesso: Roubo/Imitação de Token (T1134.001)	Execução Acionada por Evento: Modificação da Configuração de Unix Shell (T1546.004)
Injeção de Processo: Injeção de biblioteca de vínculo dinâmico (T1055.001)	Contas Válidas: Contas de Domínio (T1078.002)
Contas Válidas: Contais Locais (T1078.003)	

Evasão de Defesa (TA0005)	
Rootkit (T1014)	Execução de Comando Indireto (T1202)
Ficheiros ou Informação Ofuscados (T1027)	System Binary Proxy Execution: Mshta (T1218.005)
Ficheiros ou informações ofuscados: Embalagem de Software (T1027.002)	System Binary Proxy Execution: Regsvr32 (T1218.010)
Ficheiros ou informações ofuscados: Esteganografia (T1027.003)	Subverter Controlos de Confiança: Assinatura de Código (T1553.002)
Ficheiros ou informações ofuscados: Compilar após a Entrega (T1027.004)	Modificações de Permissões de ficheiro e diretório: Modificações de Permissões de ficheiro e diretório Linux and Mac (T1222.002)
Disfarce: Corresponder nome ou local legítimo (T1036.005)	Virtualização/Evasão de Sandbox: Verificações do sistema (T1497.001)
Injeção de Processo: Sequestro de Execução de Thread (T1055.003)	Disfarce (T1036)
Carregamento de Código Reflexivo (T1620)	Prejudicar as defesas: Disativar ou Modificar o Firewall do Sistema (T1562.004)
Injeção de Processo: Escavação de Processo (T1055.012)	Ocultar Artefactos: Arquivos e Diretórios Ocultados (T1564.001)
Remoção do Indicador: Exclusão de ficheiro (T1070.004)	Ocultar Artefactos: Janela Oculta (T1564.003)
Remoção do Indicador: Timestomp (T1070.006)	Fluxo de Execução de Sequestro: Sequestro de ordem de pesquisa de DLL (T1574.001)
Remoção do Indicador: Limpar Registos de Eventos do Windows (T1070.001)	Fluxo de Execução de Sequestro: Carregamento lateral do DLL (T1574.002)
Modificar Registo (T1112)	Serviço Web (T1102)
Desofuscar/Decodificar Ficheiros ou Informação (T1140)	Disfarce: Disfarçar Tarefa ou Serviço (T1036.004)
Prejudicar as defesas (T1562)	

Acesso às credenciais (TA0006)	
Despejo de credenciais do sistema operacional: Memória LSASS (T1003.001)	Credenciais sem garantia: Credenciais nos ficheiros (T1552.001)
Despejo de credenciais do sistema operacional: NTDS (T1003.003)	Força Bruta: Adivinhar palavra-passe (T1110.001)
Sniffing de Rede (T1040)	Autenticação Forçada (T1187)

Acesso às credenciais (TA0006)	
Credenciais de Armazenamentos de palavras-passe: Gestor de palavras-passe (T1555.001)	Roubar ou Falsificar Bulhetes Kerberos: Kerberoasting (T1558.003)
Captura de entrada: Keylogging (T1056.001)	Interceptação de Autenticação Multifactor (T1111)
Roubar Cookie de Sessão de Web(T1539)	Roubar Token de Acesso à Aplicação (T1528)
Exploração para Acesso a Credenciais (T1212)	Força Bruta: Quabra de palavra-passe (T1110.002)
Captura de entrada: Captura de Portal de Web (T1056.003)	Despejo de credenciais do sistema operacional: DCSync (T1003.006)
Credenciais de Armazenamentos de palavras-passe (T1555)	Credenciais de Armazenamentos de palavras-passe: Credenciais de Navegadores da Web (T1555.003)

Descoberta (TA0007)	
Descoberta de Serviço do Sistema (T1007)	Descoberta de Informação do Sistema (T1082)
Descoberta de Janela de Aplicação (T1010)	Descoberta de Conta: Conta Local (T1087.001)
Consultar Registo (T1012)	Descoberta de Informação do Sistema, Técnica T1082 - Empresa | MITRE ATT&CK®
Descoberta de Ficheiro e Diretório (T1083)	Descoberta do Horário do Sistema (T1124)
Descoberta de Serviço de Rede (T1046)	Descoberta do Proprietário/Utilizador do Sistema (T1033)
Descoberta do Sistema Remoto (T1018)	Descoberta de Confiança de Domínio (T1482)
Descoberta de Conta: Conta Eletrónica (T1087.003)	Descoberta de Conta: Conta de Domínio (T1087.002)
Descoberta de Conexões de Rede do Sistema (T1049)	Evasão de Virtualização/Sandbox: Verificações do sistema (T1497.001)
Descoberta de Processo (T1057)	Descoberta de Software (T1518)
Descoberta de Grupos de Permissão: Grupos de Domínio (T1069.002)	Descoberta de Partilha de Rede, Técnica T1135 - Empresa | MITRE ATT&CK®
Descoberta de Configuração de Rede do Sistema: Descoberta de Conexão de Internet (T1016.001)	

Movimento Lateral (TA0008)	
Serviços Remotos: Protocolo de Área de Trabalho Remota (T1021.001)	Remote Services (T1021)
Serviços Remotos: Partilhas Administrativas SMB/ Windows (T1021.002)	Utilizar Material de Autenticação Alternativo: Passe o Bilhete (T1550.003)
Serviços Remotos: Gestão Remota de Windows (T1021.006)	Transferência Lateral de Ferramenta (T1570)

Recolha (TA0009)	
Dados do Sistema Local (T1005)	Arquivar Dados Recolhidos: Arquivar através da Biblioteca (T1560.002)
Dados da Pasta de Rede Partilhada (T1039)	Recolha de emails: Recolha Remota de emails (T1114.002)

Recolha (TA0009)	
Captura de entrada: Keylogging (T1056.001)	Dados da Área de Transferência (T1115)
Recolha Automatizada (T1119)	Dados de Repositórios de Informação (T1213)
Captura de entrada: Captura de Portal da Web (T1056.003)	Dados Preparados: Preparação Remota de Dados (T1074.002)
Dados Preparados: Preparação de Dados Locais (T1074.001)	Arquivar Dados Recolhidos (T1560)
Recolha de emails (T1114)	

Exfiltração (TA0010)	
Exfiltração acima do Canal C2 (T1041)	Exfiltração acima do Protocolo Alternativo: Exfiltração acima do Protocolo Não-C2 Encriptado Assimétrico (T1048.002)
Exfiltração acima do Protocolo Alternativo (T1048)	Exfiltração acima do Serviço Web: Exfiltração para Armazenamento em Nuvem (T1567.002)

Comando e Controlo (TA0011)	
Ofuscação de Dados: Imitação de Protocolo (T1001.003)	Serviço da Web: Dead Drop Resolver (Solucionador de problemas) (T1102.001)
Porta Frequentemente Utilizada (T1043)	Serviço da Web: Comunicação Unilateral (T1102.003)
Protocolo da camada de aplicação: Protocolos da Web (T1071.001)	Transferência de Ferramenta de Entrada (T1105)
Protocolo da camada de aplicação: Protocolos de Transferência de Ficheiros (T1071.002)	Proxy: Proxy Interno (T1090.001)
Proxy: Proxy Externo (T1090.002)	Porta Não-Padrão (T1571)
Proxy: Proxy Multi-hop (T1090.003)	Tunelamento de Protocolo (T1572)
Serviço da Web: Comunicação Bidirecional (T1102.002)	Canal Encriptado (T1573)
Canal Encriptado: Criptografia Assimétrica (T1573.002)	Transferência de Ferramenta de Entrada (T1105)
Proxy, Técnica T1090 - mpresa | MITRE ATT&CK®	

Impacto (TA0040)	
Interrupção do Serviço (T1489)	Apagar Disco (T1561)
Desligamento/Reinicialização do Sistema (T1529)	Sequestro de Recursos (T1496)

Notas

Isenção de responsabilidade

O conteúdo deste guia é de natureza geral e não deve ser considerado como aconselhamento jurídico, nem utilizado como referência em circunstâncias específicas ou situações de emergência. Em qualquer assunto importante, deve procurar o aconselhamento profissional independente adequado em relação às suas circunstâncias pessoais.

A Commonwealth não se responsabiliza por quaisquer danos, perdas ou despesas incorridos como resultado da confiança nas informações contidas neste guia.

Para mais informação ou para relatar um incidente de segurança cibernética, contacte-nos:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Este número está disponível para uso apenas dentro da Austrália.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre